



blacklens.io

Blick durch die Brille des ANGREIFERS

a service by © snapSEC GmbH

snapSEC. keep it simple and effective

WHO WE ARE



Michael KARL
michael.karl@snapsec.at
+43-664-828-4747

knapp 20 Jahre an der Schnittstelle von Cybersecurity, Angriff und Verteidigung mit Schwerpunkten:

- **Attack Surface Monitoring**
- Offensive/Defensive Security
- Cyber-Resilienz

Co-Founder snapSEC GmbH

Hersteller der **ASM-Plattform** blacklens.io

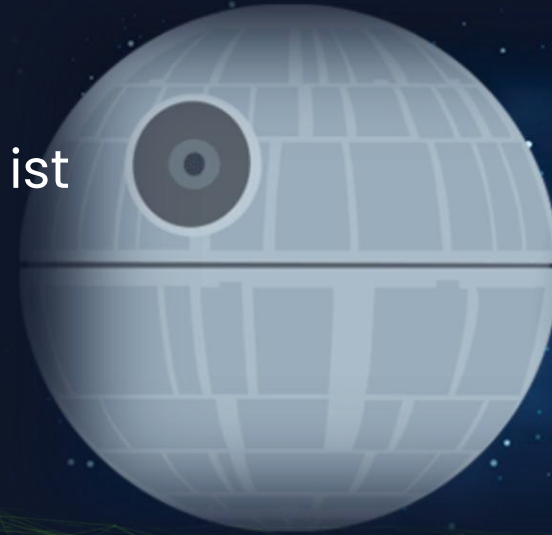
Anbieter von **Active Cyber Defense Services** (MDR/SOC)

VORBEREITET ZU SEIN IST EINFACH, WENN MAN EINEN GUTEN PLAN HAT!

Agenda

Attack Surface Reduction & Darknet Monitoring

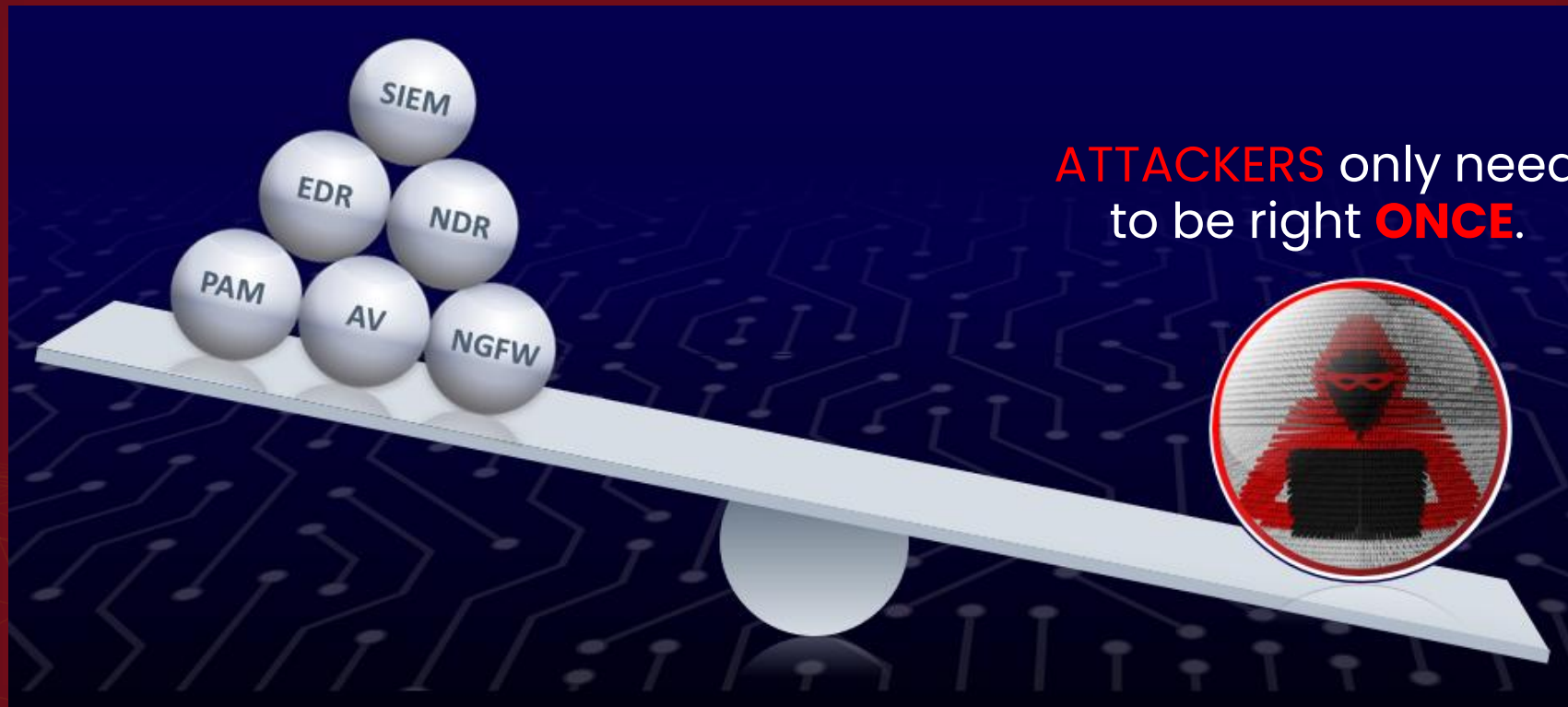
- ❖ Einführung in **Attack Surface Management (ASM)**
- ❖ **Attack Surface Reduction** – wie viel ist genug?
- ❖ **Darknet Monitoring** – was es ist und was es nicht ist
- ❖ Zusammenspiel von **ASM & Darknet Monitoring**
- ❖ Praxisnahe **Use Cases** aus Unternehmen
- ❖ Governance, Prozesse & Verantwortlichkeiten
- ❖ Fragen & Diskussion (**Q&A**)



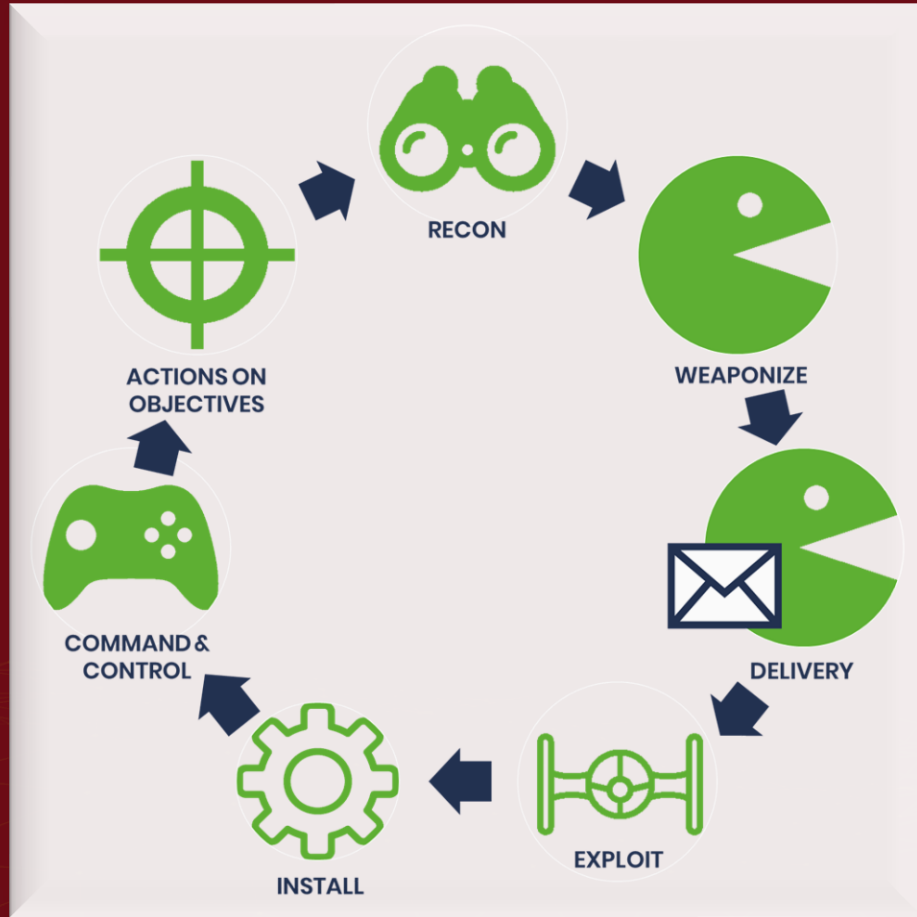
WITH
CYBERSECURITY

Einführung in Attack Surface Management (ASM)

DEFENDERS need to be
right **EVERY TIME**.



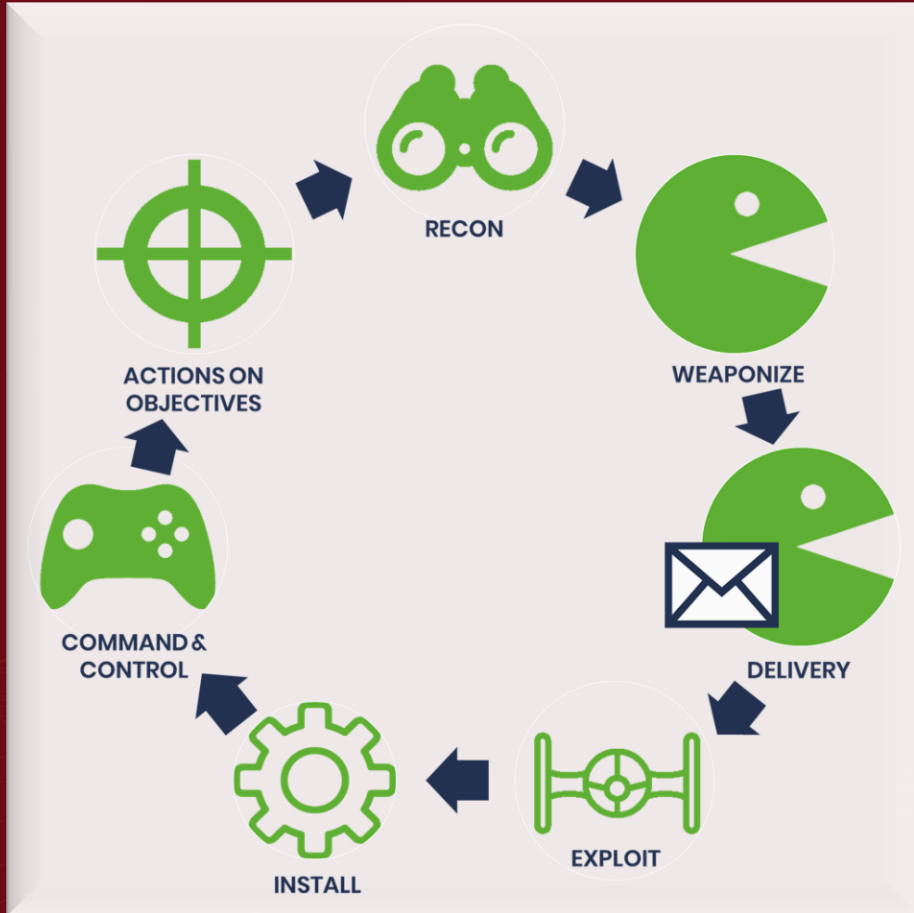
Einführung in Attack Surface Management (ASM)



360° Cybersicherheit



Einführung in Attack Surface Management (ASM)



360° Cybersicherheit

- **Prävention** – *wie schützt man Bekanntes vor Bekanntem?*
- **Detektion** – *wie erkennt man, was dennoch durchkommt?*
- **Reaktion** – *wie und wie schnell reagiert man?*

Einführung in Attack Surface Management (ASM)

Organisationen unterschätzen oft, wie
groß ihre Angriffsfläche eigentlich ist

- ❖ Intern, Extern, Cloud, Entra ID (AAD), GCP, AWS,...
- ❖ Domains, Subdomains, Cloud-Services, APIs,...
- ❖ Endpoints, Service-User, Crown Jewels,...
- ❖ Mitarbeiter, Admins, Third Parties, Supply Chain,...



Einführung in Attack Surface Management (ASM)



❖ **Identify**

- ❖ über welche Assets verfügen wir?
- ❖ wo haben wir blinde Flecken?

❖ **Assess**

- ❖ welche Risiken gehen davon aus?
- ❖ Exponierung, Kritikalität, Kontext
- ❖ nicht alles ist gleich wichtig

❖ **Prevent**

- ❖ Reduzieren, absichern, abschalten
- ❖ TOM
- ❖ kontinuierliches Monitoring

Attack Surface Reduction wie viel ist genug?

Vollständige Attack Surface Reduction ist eine Illusion

- ❖ Attack Surface verändert sich ständig
- ❖ Third Parties erweitern die Angriffsfläche außerhalb der eigenen Kontrolle
- ❖ Menschliches Verhalten erzeugt immer neue Risiken
- ❖ "Unbekannte Unbekannte" lassen sich nicht vollständig eliminieren



Attack Surface Reduction wie viel ist genug?

Wo Attack Surface Management oft scheitert

- ❖ Fokus nur auf Tools statt auf Prozesse
- ❖ keine klare Ownership
- ❖ keine Priorisierung wegen zu vieler Findings
- ❖ keine Verbindung Business Risiken / Impact
- ❖ ASM als einmaliges Projekt statt als Prozess

Attack Surface Reduction wie viel ist genug?



Weg vom "alles absichern Denken" – hin zu risikobasierter Angemessenheit

Darknet Monitoring was es ist und was es nicht ist

Was haben John Wick und das Darknet gemeinsam?

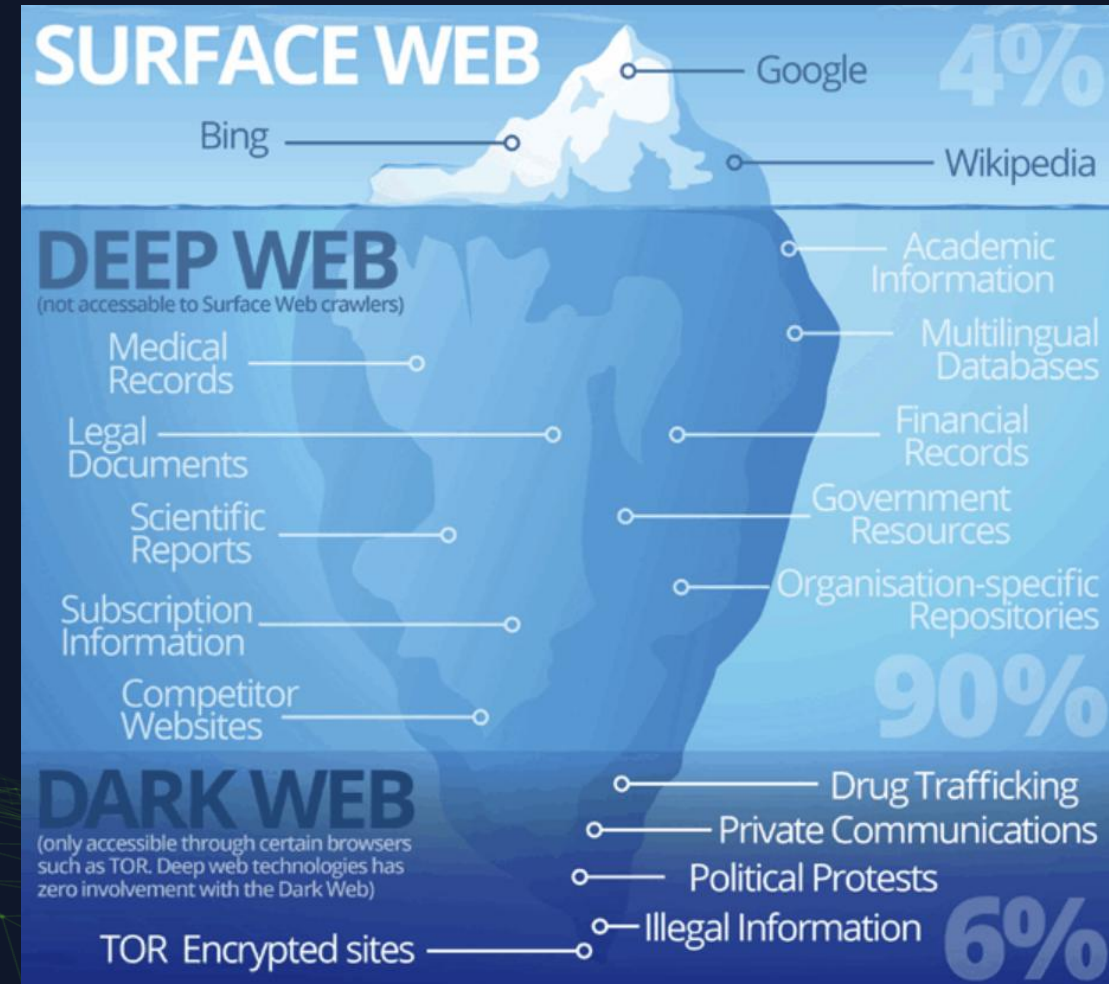
- ❖ Ein exklusiver Ort – nicht öffentlich zugänglich
- ❖ Zugang basiert auf Vertrauen und Reputation
- ❖ Die wirklich relevanten Geschäfte finden nicht im Erdgeschoss statt



Darknet Monitoring was es ist und was es nicht ist

Warum Monitoring so schwierig ist, lässt sich gut anhand des Continental Hotels erklären.

- ❖ **Erdgeschoss / Lobby** (Leak Dumps, veraltete Breaches, öffentliche Paste-Sites)
- ❖ **Obere Etagen** (geschlossene Foren, Initial Access Broker, exklusive Market-Places)
- ❖ **Zutritt** (auf Einladung und Reputation)



Darknet Monitoring was es ist und was es nicht ist

Die große Illusion des Darknet Monitorings

- ❖ Darknet ist kein indexierbarer Raum
- ❖ Foren sind geschlossen und temporär
- ❖ Zugang meist auf Einladung durch Vertrauen und Interaktionen



Darknet Monitoring was es ist und was es nicht ist

Ist Darknet Monitoring nur ein Hype?

- ❖ **WE HAVE MFA** – Identitätsdiebstahl ist für uns kein Problem
- ❖ **WE HAVE XDR** – dass wir Threats nicht detektieren ist unwahrscheinlich
- ❖ **WE HAVE CASB** – kritische Daten können die Firma nicht verlassen



Darknet Monitoring

was es ist und was es nicht ist

Was es **leisten kann**

- Frühe Warnsignale liefern
- Fehlkonfigurationen sichtbar machen
- Kontext für ASM und IR liefern

Was es **nicht leisten kann**

- Angriffe verhindern
- Vollständigkeit garantieren
- Prozesse ersetzen

Darknet Monitoring ist ein Sensor – KEIN Schutzschild

Darknet Monitoring was es ist und was es nicht ist

5 Punkte, die Sie vor einer Investition klären sollten

- ❖ Klare Zielsetzung definieren
- ❖ Tiefe und operative Fähigkeiten erfragen
- ❖ Test statt Versprechen
- ❖ Vorsicht bei sensiblen Daten
- ❖ Klare Reaktionsprozesse



Zusammenspiel ASM und Darknet Monitoring

Attack Surface Management

- Zeigt: was ist exponiert, was ist angreifbar
- Fokus: Assets, Konfigurationen, Sichtbarkeit
- Blick von aussen nach innen

Darknet Monitoring

- Zeigt: was wird bereits missbraucht
- Fokus: Daten, Zugänge, Identitäten
- Blick aus dem Underground auf das Unternehmen

ASM zeigt die Angriffsfläche – Darknet Monitoring zeigt die Nutzung dieser Fläche

Zusammenspiel ASM und Darknet Monitoring



Typischer Praxisfall

- ❖ ASM: Subdomain mit Login-Seite entdeckt
- ❖ Darknet: Zugangsdaten der selben Domain im Umlauf
- ❖ Ergebnis
 - ❖ Risiko ist klar
 - ❖ Priorität hoch
 - ❖ Maßnahme eindeutig

Use Case

Attack Surface Management

Sichtbarkeit & Priorisierung

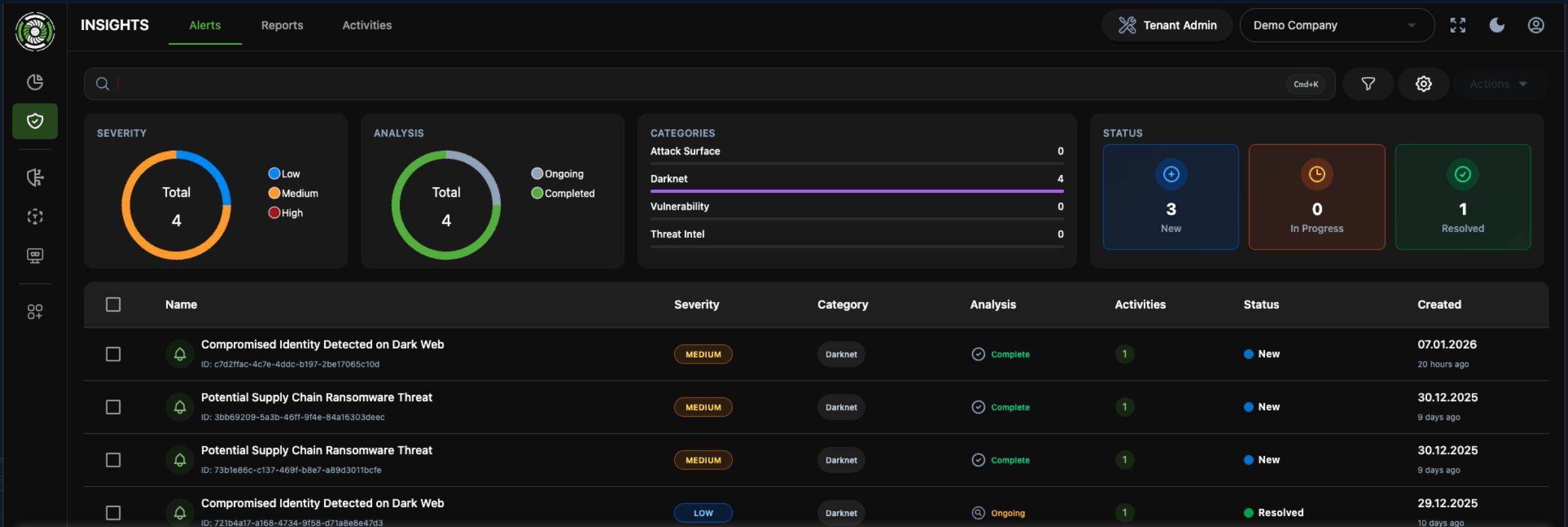
- ❖ Asset Inventory / Identifizierung relevanter Assets
- ❖ ganzheitliche Visualisierung der Angriffsfläche
(extern, intern, Cloud, Subdomains, Test-/Projekt-Systeme, Supply Chain...)
- ❖ Autonomous Attack Surface Discovery
- ❖ Bewertung / Tagging nach Kontext
(Kritikalität, sensible Funktionen, Vorbereitung Übersicht für Schnelle Reaktionsfähigkeit)



You can't protect what you don't know

Use Case

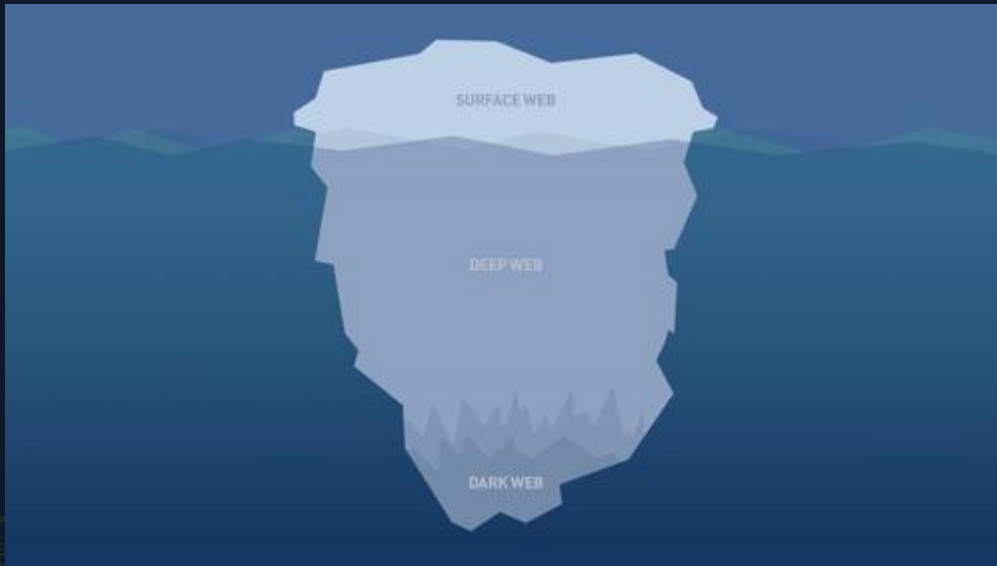
Attack Surface Management



- ❖ Kritische Bedrohungen auf einem Blick
- ❖ Maßnahmen gezielt priorisieren und abarbeiten
- ❖ Erkennung aufkommender Bedrohungen in nahezu Echtzeit für schnelle Handlungsfähigkeit

Use Case

ASM + Darknet Monitoring in der Praxis



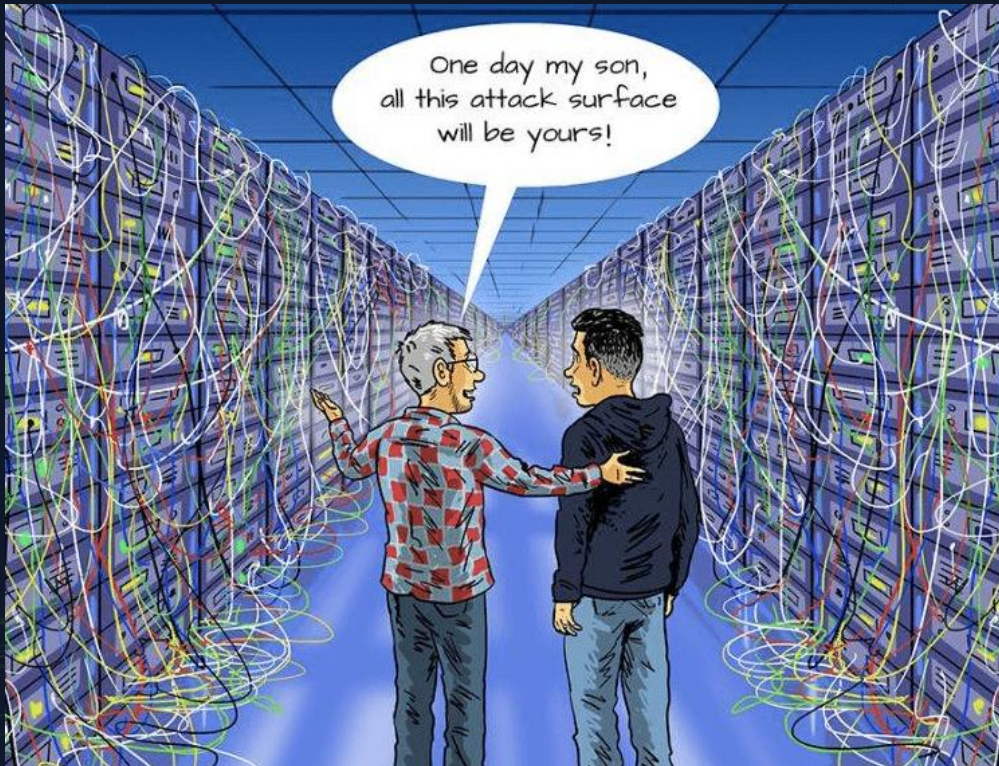
Darknet-Perspektive auf Session Cookies

- ❖ Account Takeover
- ❖ **Session / Renewal Cookie**
- ❖ Stealer
- ❖ Ableitbare Hinweise und Rückschlüsse
(ist bereits etwas passiert, Quelle des Leaks, direkt oder indirekt / **Lieferkette**)

Darknet Leaks für sich interessant, aber schwerer einzuordnen

Use Case

ASM + Darknet Monitoring in der Praxis



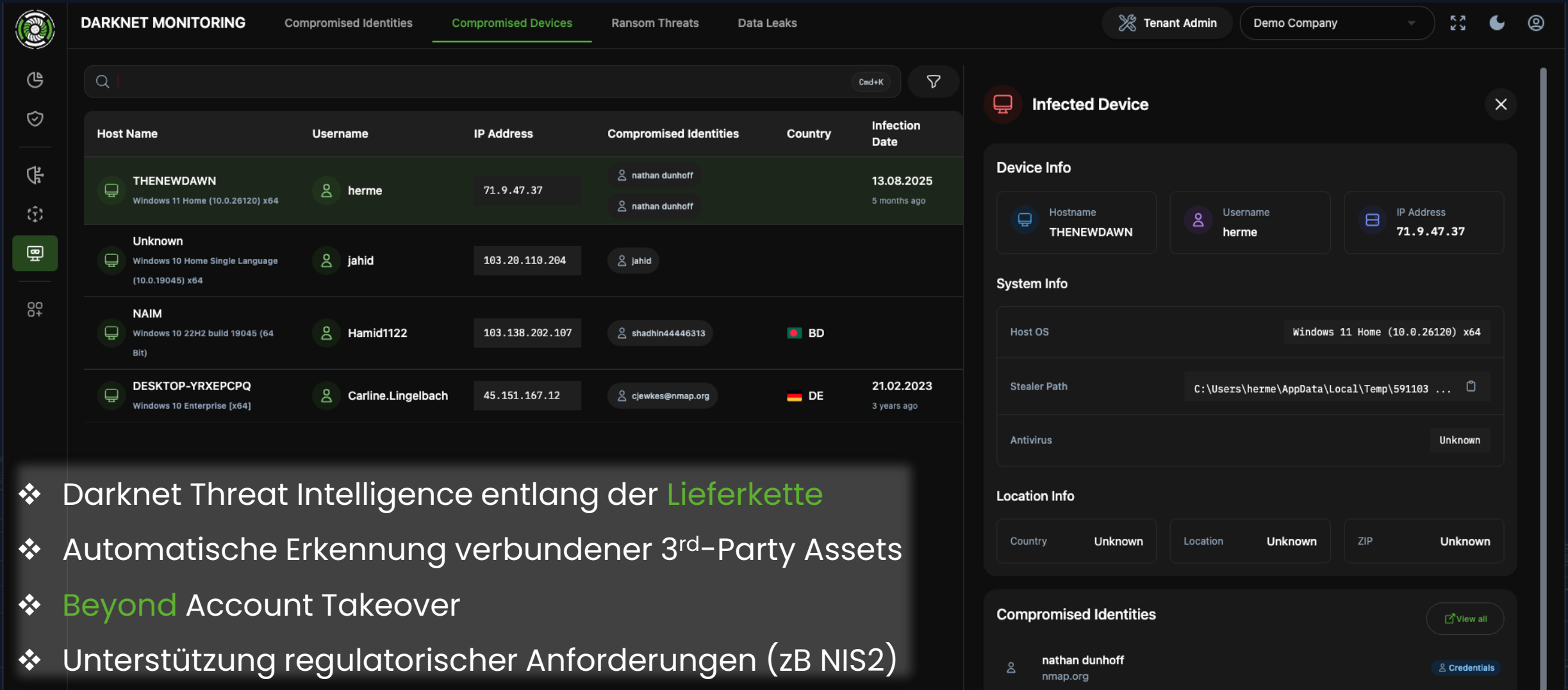
ASM-Perspektive auf Session Cookies

- ❖ Welche Admin-Interfaces existieren
- ❖ Wo sind sie erreichbar
- ❖ Wie kritisch sind sie
- ❖ Welche Schutzmechanismen existieren
- ❖ Wie sind Policies deployed

ASM zeigt, wo Session Leaks gefährlich wären

Use Case

ASM + Darknet Monitoring in der Praxis



The screenshot displays the BlackLens.io Darknet Monitoring interface. The main navigation bar includes 'DARKNET MONITORING', 'Compromised Identities', 'Compromised Devices' (active), 'Ransom Threats', and 'Data Leaks'. The user is logged in as 'Tenant Admin' for 'Demo Company'. The main content area shows a table of compromised devices with columns for Host Name, Username, IP Address, Compromised Identities, Country, and Infection Date.

Host Name	Username	IP Address	Compromised Identities	Country	Infection Date
THENEWDAWN Windows 11 Home (10.0.26120) x64	herme	71.9.47.37	nathan dunhoff nathan dunhoff		13.08.2025 5 months ago
Unknown Windows 10 Home Single Language (10.0.19045) x64	jahid	103.20.110.204	jahid		
NAIM Windows 10 22H2 build 19045 (64 Bit)	Hamid1122	103.138.202.107	shadhin44446313	BD	
DESKTOP-YRXEPCPQ Windows 10 Enterprise [x64]	Carline.Lingelbach	45.151.167.12	cjewkes@nmap.org	DE	21.02.2023 3 years ago

The right sidebar shows a detailed view of an 'Infected Device' with the following information:

- Device Info:** Hostname: THENEWDAWN, Username: herme, IP Address: 71.9.47.37
- System Info:** Host OS: Windows 11 Home (10.0.26120) x64, Stealer Path: C:\Users\herme\AppData\Local\Temp\591103..., Antivirus: Unknown
- Location Info:** Country: Unknown, Location: Unknown, ZIP: Unknown
- Compromised Identities:** nathan dunhoff (nmap.org) with a 'View all' link and a 'Credentials' link.

- ❖ Darknet Threat Intelligence entlang der Lieferkette
- ❖ Automatische Erkennung verbundener 3rd-Party Assets
- ❖ Beyond Account Takeover
- ❖ Unterstützung regulatorischer Anforderungen (zB NIS2)

Use Case

Vulnerability Management im Kontext von ASM

VM ohne Kontext: Viele Schwachstellen – wenig Klarheit

- ❖ regelmäßige Scans
- ❖ Hunderte / Tausende Findings
- ❖ CVSS als Hauptkriterium
- ❖ begrenzte Ressourcen



Use Case

Vulnerability Management im Kontext von ASM

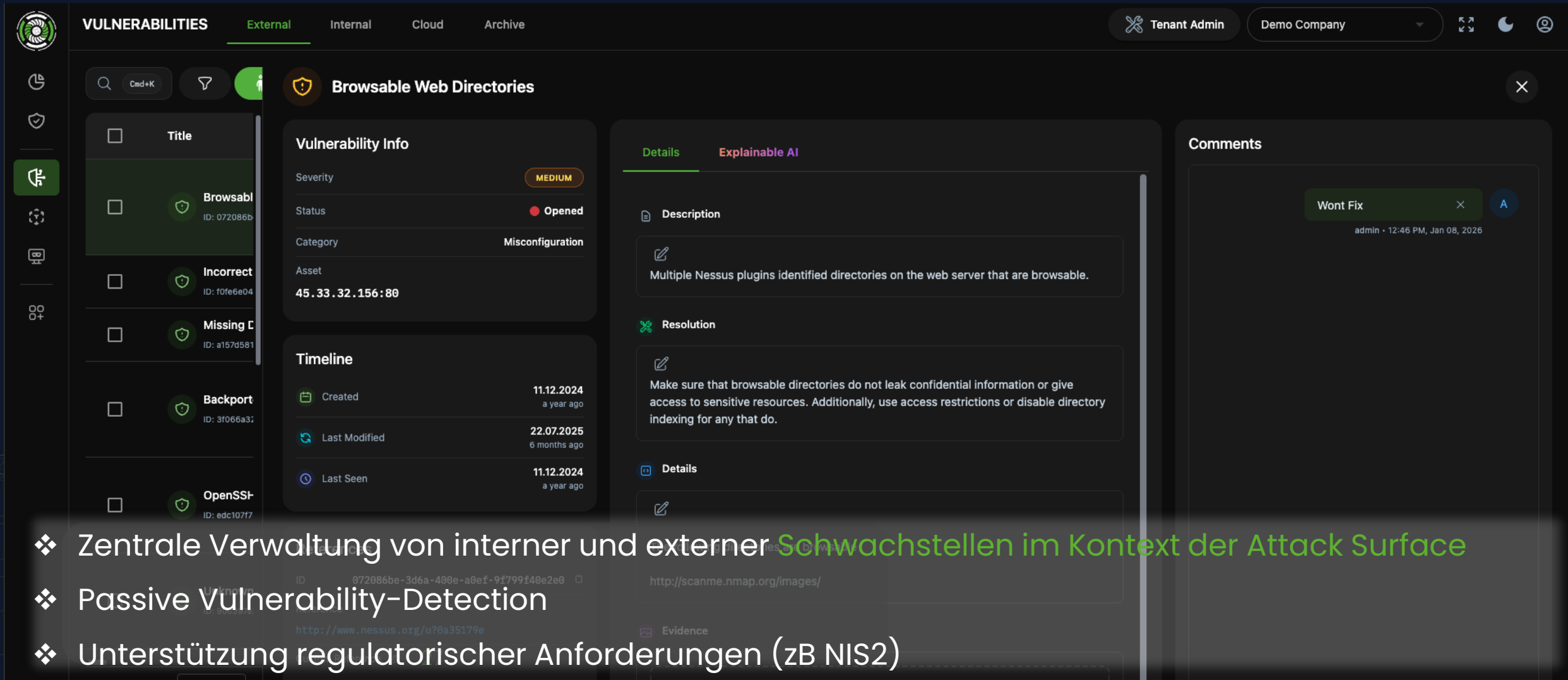
VM mit ASM-Kontext: Warum kritisch \neq kritisch ist

- ❖ regelmäßige Scans
- ❖ Hunderte / Tausende Findings
- ❖ CVSS als Hauptkriterium
- ❖ begrenzte Ressourcen



Use Case

Vulnerability Management im Kontext von ASM



The screenshot displays the 'VULNERABILITIES' dashboard in the 'External' view. The main focus is on a vulnerability titled 'Browsable Web Directories' with a severity of 'MEDIUM' and a status of 'Opened'. The interface includes a search bar, a filter icon, and a list of other vulnerabilities such as 'Incorrect', 'Missing C', 'Backport', and 'OpenSSH'. The details panel for the selected vulnerability shows a description: 'Multiple Nessus plugins identified directories on the web server that are browsable.' and a resolution: 'Make sure that browsable directories do not leak confidential information or give access to sensitive resources. Additionally, use access restrictions or disable directory indexing for any that do.' A 'Comments' section shows a note 'Wont Fix' from 'admin' on 'Jan 08, 2026'. The bottom of the image features three bullet points in German.

- ❖ Zentrale Verwaltung von interner und externer Schwachstellen im Kontext der Attack Surface
- ❖ Passive Vulnerability-Detection
- ❖ Unterstützung regulatorischer Anforderungen (zB NIS2)

Governance, Prozesse und Verantwortlichkeiten

❖ **Wer ist verantwortlich?**

- ❖ Product Owner definieren
- ❖ wer legt Prioritäten fest
- ❖ wer darf abschalten, härten, reagieren

❖ **Wie wird entschieden?**

- ❖ was ist kritisch?
- ❖ was ist beobachtenswert?
- ❖ was wird bewusst akzeptiert?

❖ **Was passiert nach einem Fund?**

- ❖ klar definierte Reaktionspfade / Playbooks
- ❖ Verbindung zu Incident Response, Vulnerability Management, IAM

The Attack Surface Management Platform



- ❖ Made in Europe
- ❖ 24x7 Echtzeit Frühwarnsystem vor Cyberbedrohungen
- ❖ Dark Web Intelligence
- ❖ Schwachstellen Management
- ❖ Penetration Testing Service

blacklens.io – Big Picture

made in Europe

eXtended Attack
Surface Monitoring



THANK YOU



TIME NOW FOR QA

Michael KARL
michael.karl@snapsec.at
+43-664-828-4747

<https://blacklens.io>